

## SECURE SYSTEM FOR ACTIVATING PERSONAL COMPUTER SOFTWARE AT REMOTE LOCATIONS

**Patent number:** JP6501120T

**Publication date:** 1994-01-27

**Inventor:**

**Applicant:**

**Classification:**

**- international:** G06F13/00; G06F15/00; H04L9/00; H04L9/00;  
H04L9/10; H04L9/12

**- european:** G06F1/00N7R2; G06F9/445; G06F9/445N;  
G06F21/00N7P5M

**Application number:** JP19910501845T 19911106

**Priority number(s):** US19900610037 19901107; US19910682456 19910409

**Also published as:**

WO9209160 (A1)  
EP0556305 (A1)  
US5222134 (A1)  
EP0556305 (A4)  
EP0556305 (B1)

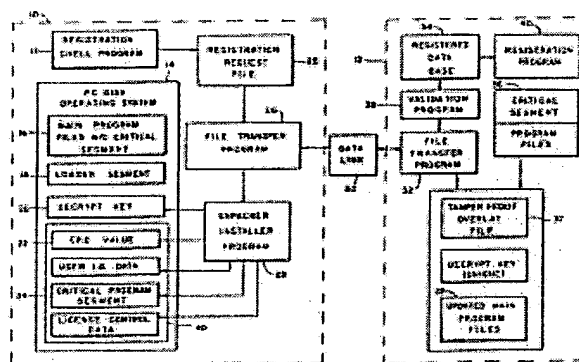
more >>

Report a data error here

Abstract not available for JP6501120T

Abstract of corresponding document: **US5222134**

A process and system for activating various programs are provided in a personal computer. The computer is initially provided with a registration shell. A data link is established between the personal computer and a registration computer. By providing the registration computer with various information, a potential licensee can register to utilize the program. Once the registration process is complete, a tamperproof overlay program is constructed at the registration computer and transferred to the personal computer. The tamperproof overlay includes critical portions of the main program, without which the main program would not operate and also contains licensee identification and license control data.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平6-501120

第6部門第3区分

(43) 公表日 平成6年(1994)2月3日

(51) Int. Cl. <sup>3</sup>	識別記号	序内整理番号	F I
G 0 6 F 13/00	3 5 1 H	7368-5B	
15/00	3 3 0 A	7459-5L	
H 0 4 L 9/00			
9/10			
	7117-5K	H 0 4 L 9/00	Z
	審査請求 有	予備審査請求 有	(全 8 頁) 最終頁に続く

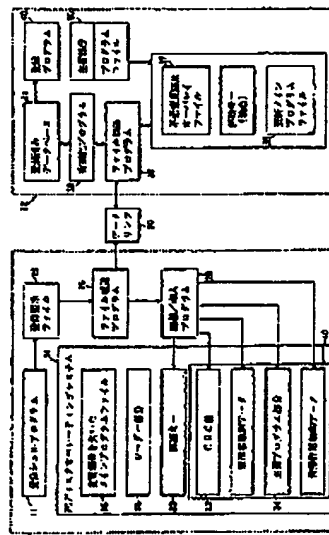
(21) 出願番号 特願平4-501845  
 (86) (22) 出願日 平成3年(1991)11月6日  
 (85) 翻訳文提出日 平成5年(1993)5月7日  
 (86) 国際出願番号 P C T / U S 9 1 / 0 8 0 6 9  
 (87) 国際公開番号 W O 9 2 / 0 9 1 6 0  
 (87) 国際公開日 平成4年(1992)5月29日  
 (31) 優先権主張番号 6 1 0 , 0 3 7  
 (32) 優先日 1990年11月7日  
 (33) 優先権主張国 米国 (U S)  
 (31) 優先権主張番号 6 9 2 , 4 5 6  
 (32) 優先日 1991年4月9日  
 (33) 優先権主張国 米国 (U S)

(71) 出願人 タウ システム コーポレーション  
 アメリカ合衆国 バージニア州 フォルス  
 チャーテ, リースバーグ バイク,  
 7115, スーツ327  
 (72) 発明者 ワイト, デービット, ビー  
 アメリカ合衆国 バージニア州 22032,  
 フェアファックス ギルバートソン ロード,  
 4220  
 (72) 発明者 リッデル, ホレイス, ジー  
 アメリカ合衆国 バージニア州 22021,  
 チャンチリイ, バレイ カウントリ ドラ  
 イブ, 13811  
 (74) 代理人 弁護士 倉持 裕 (外1名)  
 最終頁に続く

(54) 【発明の名称】 パーソナルコンピュータのソフトウェアを遠隔位置で起動するための安全システム

## (57) 【要約】

様々なプログラムを起動するための過程とシステムがパーソナルコンピュータ(10)に提供されている。パーソナルコンピュータ(10)には、登録シェルスプログラム(11)が当初備わっている。データリンク(20)がパーソナルコンピュータ(10)と登録用コンピュータ(12)の間に確立される。登録用コンピュータ(12)に様々な情報を与えることにより、見込み被許諾者はメインプログラム(16)の使用を登録することができる。ひとたび登録過程が完了すると、不正変更防止オーバーレイプログラムが登録用コンピュータ(12)において作成され、パーソナルコンピュータ(10)に転送される。不正変更防止オーバーレイには、メインプログラム(16)の主要部分がふくまれ、これを欠くとメインプログラム(16)は動作せず、また不正変更防止オーバーレイには使用許諾識別データと使用許諾制御データも含まれている。



## 特実平6-501120 (2)

暗号化オーバーレイファイル内にあるとともに、解放キーを上記オーバーレイファイルに格納する請求の範囲第1項に記載の方法。

6. 上記オーバーレイが実行のためにロードされるたびに返戻冗長検査値が計算され、上記不正変更防止オーバーレイファイル内に格納された返戻冗長検査値と比較され、上記オーバーレイファイルが加減後変更されているかどうかを判断することと特徴とする請求の範囲第4項に記載の方法。

6. 上記使用者識別情報と上記オーバーレイファイルとが、電子データリンクを介して上記登録シェルと上記登録プログラムとの間を伝送されることを特徴とする請求の範囲第1項に記載の方法。

7. 上記登録シェルプログラムが、上記登録した登録用コンピュータを備えた第二の遠隔コンピュータから離れた、第一のコンピュータ内に格納されていることを特徴とする請求の範囲第1項に記載の方法。

8. 上記利用可能工程によって上記使用者識別情報が正式の登録シェルを確保することを特徴とする請求の範囲第2項に記載の方法。

9. 上記使用者識別と上記オーバーレイファイルが、一台のコンピュータに入力され備えられることを特徴とする請求の範囲第1項に記載の方法。

10. プログラムファイルを制御せられたりしくは制御されない期間を助するためのシステムにおいて、

オーバーレイローダー部分が含まれているが少なくとも一つの

13. オーバーレイファイルを作成するための上記手段が、返戻冗長検査値を備える不正変更防止オーバーレイファイルを作成するための暗号化値と解放キーを備えており、上記解放キーは上記オーバーレイファイルと共に上記遠隔コンピュータに伝送されることを特徴とする請求の範囲第10項に記載のプログラムファイル制御システム。

14. 上記遠隔コンピュータが、上記オーバーレイファイルを解放し、上記オーバーレイファイルが実行のためにロードされるたびに返戻冗長検査値を計算し、そしてこの検査値を上記登録用コンピュータによって上記オーバーレイファイルと共に伝送された返戻冗長検査値と比較するための手段を備えていることを特徴とする請求の範囲第12項に記載のプログラムファイル制御システム。

15. 上記主要部分がエグゼクティブ制御部分であり、そして上記使用者識別情報が使用許諾契約情報であることを特徴とする請求の範囲第1項に記載の方法。

16. 上記主要プログラム部分のエグゼクティブ制御プログラムであり、そして上記使用者識別情報が使用許諾契約情報であることを特徴とする請求の範囲第10項に記載のプログラムファイル制御システム。

17. 上記主要エグゼクティブ制御プログラム部分がプログラムファイル全体を有することを特徴とする請求の範囲第16項に記載のプログラムファイル制御システム。

18. プログラムファイルの使用を制御する方法において、表示装置を有するコンピュータに対してローダー部分と登録シェル部分を含むプログラムファイルを提供し、上記プログラムフ

## 【請求の範囲】

1. プログラムファイルを格納する方法であって、

表示装置を有する遠隔コンピュータに対して、ローダーセグメントと登録シェル部分を含むプログラムファイルを提供し、上記プログラムファイルは主要部分が欠いて、上記プログラムファイルを正しく実行することを阻止する工程、

使用者識別情報と上記登録シェル部分を入力する工程、

上記使用者識別情報を、上記登録シェルから登録用コンピュータ内にある格納した登録プログラムに格納し、上記登録プログラムは使用者識別データと上記登録部分を結合して独自のオーバーレイファイルを作成する工程、

上記独自のオーバーレイファイルを上記登録プログラムから上記登録シェルに格納する工程、上記オーバーレイファイルには上記プログラムファイルには当初欠けている主要部分が含まれ、そして

上記オーバーレイファイルを上記メインプログラムファイルに格納する工程を有し、上記オーバーレイファイルに入っている使用者識別が格納されたときだけ上記プログラムファイルの動作が可能とすることを特徴とする前記のプログラムファイル制御方法。

2. 上記オーバーレイファイルを上記登録用コンピュータから上記遠隔コンピュータに伝送する前に、上記使用者識別情報を利用可能にする工程を有する請求の範囲第1項に記載の方法。

3. 不正変更防止のオーバーレイファイルを作成する工程を有する請求の範囲第1項に記載の方法。

4. 上記不正変更防止オーバーレイファイルが上記オーバーレイファイルを暗号化することにより作成され、返戻冗長検査値が上記

主要プログラム部分が欠けているプログラムファイルが当初備わっていて、このプログラムファイルが動作することを防止し、上記オーバーレイローダー部分は本物のオーバーレイファイルが現在格納されているときだけこのプログラムファイルを格納することができ、上記遠隔コンピュータには登録シェルプログラムが備えられ、上記登録シェルプログラムは使用者が様々な使用者識別情報を入力することを可能にするような少なくとも一台の遠隔コンピュータと、

登録プログラムと、上記使用者識別情報を受信し処理するための手段と、上記プログラムファイルに欠けている上記主要プログラム部分と使用者識別情報の全部あるいは一部を含む独自のオーバーレイファイルを作成するための手段と、上記オーバーレイファイルを上記遠隔コンピュータに伝送する手段とを備えた登録用コンピュータとを有し、

上記オーバーレイファイルを上記遠隔コンピュータに伝送することで、上記オーバーレイファイルに入っている使用者識別が現在格納されているときだけ上記プログラムファイルの動作が可能になることを特徴とする上記プログラムファイル制御システム。

13. 上記遠隔コンピュータと上記登録用コンピュータとの間を結合する電子データリンクと、上記登録用コンピュータと上記遠隔コンピュータの両方に備えられているファイル転送手段とを含むことを特徴とする請求の範囲第10項に記載のプログラムファイル制御システム。

14. 上記登録用コンピュータが、すべての登録済み使用者が含まれている中央データベースと上記使用者識別情報を格納化するための手段とを備えていることを特徴とする請求の範囲第10項に記載のプログラムファイル制御システム。

## 第6表平6-501120 (9)

ファイルは第二レベルの制御機能を持つエグゼクティブ制御プログラムを有しており、

情報を上記登録レベル部分に入力し、

上記使用許諾契約情報と上記登録レベルから独立登録プログラムに伝送し、上記登録プログラムは使用許諾契約データを第二レベルの制御機能を持つエグゼクティブ制御プログラムに併合して独自のオーバーレイファイルを作成し、

上記独自のオーバーレイファイルを上記登録プログラムから上記登録レベルに伝送し、上記オーバーレイファイルには上記第二レベルのエグゼクティブ制御プログラムが含まれており、そして

上記独自のオーバーレイファイルを上記登録プログラムファイルに導入し、上記プログラムファイルの第二レベルの機能の動作が上記オーバーレイファイル内の使用許諾契約情報が現在導入されていると見做されること特徴とする上記のプログラムファイル使用の制御方法。

18. 上記オーバーレイファイルを上記登録用コンピュータから上記登録コンピュータに伝送する手段に、上記使用許諾契約情報を有効化する工程を有する請求の範囲第18項に記載の方法。

19. 不正複製防止になっているオーバーレイファイルを作成する工程を有する請求の範囲第18項に記載の方法。

20. 上記不正複製防止オーバーレイファイルが上記不正複製防止オーバーレイファイルを暗号化キーで暗号化することにより作成され、巡回冗長検査値を上記暗号化不正複製防止オーバーレイファイル内に提供するとともに暗号キーを上記不正複製防止オーバーレイファイルに提供し、上記暗号化および暗号キーは上記オーバーレイファイルの独自の内容によって自由に決定されることを特徴とする請求の範囲第19項に記載の方法。

上記登録レベルプログラムは使用者が様々な使用許諾契約情報を入力することを可能にするよう少なくとも一つの登録コンピュータと、

登録プログラムと、上記使用許諾契約情報を受渡し処理するための手段と、第二レベルの機能を持つプログラムモジュールと使用許諾契約情報の全部あるいは一部を含む独自のオーバーレイファイルを作成するための手段と、上記オーバーレイファイルを上記登録コンピュータに伝送する手段とを備えた登録用コンピュータとを有し、

上記オーバーレイファイルを上記登録コンピュータに伝送することで、上記オーバーレイファイルに入っている使用許諾契約情報が現在使われているとだけ、上記プログラムファイルの第二レベルの機能動作が可能なることを特徴とする上記システム。

28. 上記登録コンピュータと上記登録用コンピュータとの間に電子データリンクを有し、ファイル転送過程が上記登録用コンピュータと上記登録コンピュータの両方に設けられていることを特徴とする請求の範囲第27項に記載のシステム。

29. 上記登録用コンピュータが、すべての登録済み使用者が全される中央データベースと上記使用許諾契約情報を有効化する手段とを備えていることを特徴とする請求の範囲第27項に記載のシステム。

30. オーバーレイファイルを作成するための上記手段が、巡回冗長検査値が記憶されている不正複製防止オーバーレイファイル作成するための暗号化キーと暗号キーとを備えており、上記暗号キーは上記オーバーレイファイルと共に上記登録コンピュータに伝送され、上記暗号化および暗号キーはファイルの内容によって自由に決定されることを特徴とする請求の範囲第27項に記載のシステム。

22. 新しい巡回冗長検査値が、上記オーバーレイが実行のためにロードされるたびに計算されて、上記オーバーレイファイルと共に伝送された巡回冗長検査値と比較され、上記オーバーレイファイルが作成以降変更されているかどうかを判断することを特徴とする請求の範囲第21項に記載の方法。

23. 上記使用許諾契約情報と上記オーバーレイファイルが、上記登録レベルと上記登録プログラムとの間で電子データリンクを介して伝送されることを特徴とする請求の範囲第18項に記載の方法。

24. 上記登録レベルプログラムが、上記独立登録プログラムを備えた第二のコンピュータから離れている第一のコンピュータに提供されていることを特徴とする請求の範囲第18項に記載の方法。

25. 上記有効化により上記使用許諾契約情報が正次の登録レベルを介して確保することを特徴とする請求の範囲第19項に記載の方法。

26. 上記使用許諾契約情報と上記オーバーレイファイルが一つのコンピュータに入力され、備えもれることを特徴とする請求の範囲第18項に記載の方法。

27. 複製されたあるいは削除されない期間、プログラムファイルとアップグレードするシステムにおいて、

第二レベルの機能を有するプログラムを含むオーバーレイローダー部分を含むプログラムファイルが自動的に、上記オーバーレイローダー部分は実際のオーバーレイファイルが現在導入されているときだけこのプログラムファイルを起動することができ、上記登録コンピュータには登録レベルプログラムが備えられ、

システム。

31. 上記登録コンピュータが、上記オーバーレイファイルを解読し、上記オーバーレイファイルが実行のためのロードされるたびに新しい巡回冗長検査値を計算し、そしてこの検査値を上記登録用コンピュータにより上記オーバーレイファイルと共に伝送された巡回冗長検査値と比較するための手段を備えていることを特徴とする請求の範囲第30項に記載のシステム。

## 【明 細 書】

パーソナルコンピュータのソフトウェアを遠隔位置で起動する  
ための資金システム

## 発明の概要

一般的に、パーソナルコンピュータあるいはそれに類似した装置の使用者の大部分は、それら装置で実行するソフトウェアを様々な小売形からあるいは遠隔販売を通じて入手する。いずれの場合も、ソフトウェア製品はいわゆる「紙箱包装」材で包装されており、その紙箱包装材を開いた時点でそのソフトウェア製品に対する使用許可契約が成立して、その製品の使用許諾者も使用許諾者/購入者による承認可能あるいは使用から保護するようになっている。この方法による商取引は、許諾者と被許諾者の双方にとって満足すべきものではないことが分かっている。たとえば、被許諾者にとっては、ソフトウェアプログラムを動作させてみてからそれが被許諾者が必要としているものかどうかを判断する機会が与えられない。さらに、許諾者の側からみると、この方法では被許諾者の識別ができないうえ、許諾者によるプログラム使用の制御あるいは監視を行なうことができない。

ソフトウェアプログラム保護方式は、Thomasの米国特許第4,448,519号に概略開示されており、プログラミングされた「はい/いいえ」で答える質問がプログラムに組み込まれており、そのソフトウェアが使用許可されるコンピュータに設置されているハードウェアあるいはファームウェア保護装置の存在を照会するようになっている。この装置の意図は、プログラムが物理的な複製をなしては使用できないようにすることであり、これはソフトウェアよりも複製することがはるかに困難である。しかし、このような装置は、正しい番号化応答が見逃され、簡単に打ち破られてしまう。ひとたび打ち破られると、無制限の違法コピーが作成され配布される可能性もある。

## 特表平6-501120 (4)

Williamの米国特許第4,740,630号は、中央（遠隔）コンピュータを介して、正しい番号の入手を試みる悪意のプログラマーがアクセスできないマスターリストあるいはアルゴリズムから導かれたコード解除コードあるいは有符号コードを提供することを開示している。しかし、この方法は、任意のコードを偽受することにより、あるいは保護の周回をプログラミングすることにより、もしくはデバッガープログラムによりプログラムを分析してプログラムの実行を可能にするコードの存在を見つけて出すことにより、簡単に見破られてしまう。ひとたびこの保護が打ち破られると、動作可能なプログラムの無制限のコピーが作成され配布される可能性がある。

さらに、Schmidtの米国特許第4,849,510号に開示されている方法では、最も価値のあるアルゴリズムを無効化し、無効化されたプログラムを処理装置内で実行すると同時に、回復アルゴリズムを別の物理的に分離した保護された処理装置で実行することにより回復し、有価価値をその処理装置の相互通信によって獲得するようになっている。このような方法は、回復アルゴリズムの物理的保護に依存しており、この物理的保護が侵害された場合、悪意のプログラマーによって簡単に打ち破られる可能性がある。したがって、そのような方法は、回復記憶媒体の物理的保護が無効でない大量市場においては、実用的ではない。

そのため、ソフトウェアを余許使用から保護しつつソフトウェアを大量市場に配布するための経済的な方法が求められる。さらに、見込み購入者/被許諾者がソフトウェア製品を購入前に試してみることができような方法とシステムも必要である。また、ソフトウェア製品の改良および更新部分と互換性用等に配布するための方法も必要である。

## 発明の簡単な説明

本発明は、パーソナルコンピュータのソフトウェアプログラムあるいは他の種類のプログラムを、使用許可を管理する方法で配

布する方法とシステムに関する。動作可能なプログラムは、購入者/被許諾者と販売者/許諾者との間の特定の契約において入手可能になる。販売者と購入者との関係は、本発明の目的に照しては、許諾者/被許諾者間の関係である必要はないが、以下では販売者を許諾者、購入者を被許諾者もしくは使用者と呼ぶ。ひとたび被許諾者が特定の契約条件に合致すると、被許諾者識別データが登録済みコンピュータに与えられる。登録済みコンピュータはその契約を記憶し、使用許可されたプログラムの可動部分を供給する。これらの部分は不正な変更防止が施されていると同時に、識別された被許諾者にとって独自のものとなっている。この情報の交換に基づき、可動コンピュータプログラムが登録済み被許諾者のコンピュータに不正な変更防止ファイルに収納されて配布される。同時に、このファイルには被許諾者独自の情報が含まれている。本発明の実施例としては様々なものが考えられるが、いずれの実施例も被許諾者を識別する独自のデータと保護されているソフトウェアプログラムに関するデータが含まれている暗号化パッケージの構成を伴っている。したがって、被許諾者は販売者ではなく、そして保護されたソフトウェアは使用許諾契約に違反できる情報で暗号化される。さらに、使用許可解除データを暗号化パッケージに含めることにより、様々な制限を課して使用許可契約の条件を遵守させることができる。

一般的に、様々な実施例は、ソフトウェアのデモンストレーション版を有する可能性のあるマーケティングシミュレーションプログラムの最初の配布に伴う。このシミュレーションプログラムは、見本版と宣伝記述だけを有しているが、あるいは完全なプログラムの動作不能版を有している。しかし、大部分の実施例は、登録プログラムと、ローセグメントと呼ばれる特定のプログラムモジュールを含むような構成になっている。

マーケティングシミュレーション方法で自由に配布されるであろう。マーケティングシミュレーションがプログラムのデモンストレーション

版を有している場合、ニグゼクティブ制御ループが保護されたプログラムの販売版になる。マーケティングシミュレーションは見込み使用者に登録を促す。マーケティングシミュレーション内の登録プログラムは、登録データと登録データベースコンピュータに接続する。暗号化ファイル内で結合された被許諾者識別データと動作可能なプログラムのプログラムとを有する独自の暗号化パッケージが組み立てられる。独自の暗号化暗号キーが、暗号化ファイルおよび保護されていないプログラムファイルと共に使用者のコンピュータに伝送される。これらはマーケットシミュレーションを最大化させる。解放キー、暗号化ファイル、そして保護されていないファイルの到着と同時に、マーケティングシミュレーションはこれらの各々を使用者のコンピュータに導入する。

したがって、使用者がプログラムを実行する毎に、ローセグメントが提供された解放キーを使用して、暗号化ファイルを保護されていないファイルに対するオーバーレイとしてロードして解放する。このプログラムは保護されていないソフトウェアプログラムの設計にしたがって実行され、独自の使用許諾データもプログラム実行中にロードされる。プログラムが実行されていないときは、保護されているプログラムはその暗号化形態に留まって、保護されていないプログラムファイルと共にコンピュータの大量記憶装置に格納されている。保護されているプログラムは実行のためにロードされたときだけ解放され、正しい暗号化キーにアクセスしなければ実行されない。

## 図面の簡単な説明

- 図1は本発明による登録過程を示す流れ図である。  
図2は本発明によるプログラム実行過程を示す流れ図である。  
図3は、本発明の知見による代表的なパーソナルコンピュータと登録済みコンピュータの構成図である。  
図4は、本発明の知見による代表的なパーソナルコンピュータと登録済みコンピュータに代る実施例を示す構成図である。

### 発明の課題と効果

本発明の目的は、許諾者がそのプログラムの費用対効果に関する調査を従来使用されている方法よりさらに効率的な方法で維持することを可能にすることである。さらに、本発明の第二の目的は、被許諾者あるいは使用者が特定のプログラムの購入あるいは使用許諾を得る前に試閲することを可能にすることである。さらに、本発明の更なる目的は、特定のプログラムの使用許諾保護されたアップグレード版を被許諾者に配布する手段を提供することである。したがって、本発明の知見は包括的なものと考えられ、そしてどのようなソフトウェアプログラムも本方法によって配布できるものと考慮されている。

一実施例において、動作可能なエグゼキュティブ制御ループを除いて完全な製品プログラムが、パーソナルコンピュータあるいは他の装置において、磁気ディスク、フロッピーディスク、ハードウェアあるいは他の手段で最初に提供される。さらに、この特定プログラムには登録シリアルプログラムも含まれる。ただし、小さいプログラムもしくは低価のあるプログラムの場合、プログラム自体は存在せず、シリアルだけが提供される。エグゼキュティブ制御ループが除外されているため、このプログラムは正しい登録過程を実現しなければ動作しない。図1および図3に示されているように、この登録過程は、パーソナルコンピュータ(PC) 10内部の登録シリアルプログラム11と登録用コンピュータ12内部に提供されている登録プログラム40とを使用して開始される。登録システムプログラムが登録用コンピュータ12内に提供され、電子データリンク30を介して登録シリアルプログラムがアクセスできる。この電子データリンクは、ローカルエリアネットワークでもよく、電話モデムリンクでもよく、あるいはその他のいかなる媒体であってもよい。ただし、第二の実施例においては、登録シリアルおよび登録システムプログラムは同一の媒体上に存在してもよいが、その媒体は製品応用プログラムとは別でなければならぬ。この場

### 特許平6-501120(5)

合、登録シリアルおよび登録システムプログラムが入っている登録可能な媒体は、許諾された購入プログラムによって使用可能なパーソナルコンピュータ10へ個人的に移植され、電子データリンクは必要ではない。

登録シリアルプログラムは、使用者がオペレーティングシステム14のメインプログラムファイル内に提供されている製品応用プログラムの実行と最初に実行すると実行される。登録シリアルは、製品応用プログラムに関する登録情報を提供しそれをPC設置位置に表示すると同時に、見込み被許諾者を監視して償却者として登録する。使用許諾は、特定の使用場面に於ける特定の被許諾者に対して提供され、その期間は何年を量るもしくは一時的でよく、そのための費用は被許諾者に対して課せられない。ただし、登録シリアルは、不正使用防止オーバーレイファイルが存在しないかどう、メインプログラムを実行しない。登録シリアルプログラム11は、被許諾者のPCに表示されるデータ入力形式を提供し、被許諾者に対して、請求書送付先、口座番号、使用許諾条件などの識別情報の提供を要求する。この情報は、被許諾者が再確認する登録要求ファイル85に入力される。そして、登録シリアルプログラムは、被許諾者が指定キーを押して登録を開始するのを待つ。このキーが押されると、登録ファイルが読み、そして登録シリアルファイル転送プログラム26が登録システムファイル転送プログラムとのデータリンクを確立する。登録用コンピュータ内の登録プログラム40は、データリンクが正当な登録シリアルで確立されていることを確認する検索保護チェックを実行する有効化手段42によって保護される。つぎに、登録シリアルは登録要求ファイル85を、そのファイルを受信する登録システムに転送し、必要なエラーチェックと、結合されたファイル転送プログラム28および92間のハンドシェイク動作を実行する。完全な登録要求ファイルが中央登録用コンピュータで受信されると、登録要求が登録購入償却者のデータベースに対して格納される。確認には、その要求に答えるべきかど

うかを判断する様々なチェックが含まれる。たとえば、一時的使用許諾に対する要求が特定の被許諾者から再度送られてきた場合、その被許諾者には使用許可が与えられ、そしてそのプログラムのエグゼキュティブ制御ループは過剰されない。そのような状態が発生した場合、適切なメッセージが登録シリアルに転送され、見込み被許諾者に対して表示される。しかし、要求が拒絶されると、登録購入使用者データベースへの登録が拒絶されるが、この過程全体が完了するまで、そのデータベースには入力されない。

登録用コンピュータ12の内部では、つぎに使用権限チェックが使用されて、使用者識別キーとエグゼキュティブ制御ループプログラム命令36とを結合することにより作成された独自の不正使用防止オーバーレイファイルが生成される。結合されたデータとプログラムファイルに基いて、不正使用防止オーバーレイファイル37内に含まれる巡回冗長検査(ECC)値が計算される。一連の独自の暗号化キーと解読キーが作成され、不正使用防止オーバーレイファイルの内容全体が暗号化キーを使用して暗号化される。この暗号化キーに基づき、不正使用防止オーバーレイファイルと共に提供される暗号化キーが提供される。暗号化アルゴリズムは、自動暗号化システムのように、暗号化と解読にそれぞれ異なるキーを使用する状態であればなんでもよい。登録システムが、不正使用防止オーバーレイファイルと解読キーを、パーソナルコンピュータ登録シリアルに伝送される1個の両行ファイル38に組み込む。また、更新されたメインプログラムファイルもこの両行ファイルに組み込まれ、ファイル転送プログラムとすでに確立されているデータリンクとを基にしてPCの登録システムに伝送される。

両行ファイル一式の受信と同時に、登録シリアルプログラム内の開閉-導入プログラム44が両行ファイルを開き、エグゼキュティブ制御ループセグメント36、CRC値22ならびに解読キー20および、含まれている場合は、更新メインプログラムファイルを含む不正使用防止オーバーレイファイル40を導入する。これで登録過程が

完了したので、電子データリンクを切断する。登録データベースレコードが入力され、そして被許諾者の要求に対する解決が、中央登録用コンピュータ12における別のプログラムによって実行される。

登録が終了すると、被許諾者のパーソナルコンピュータに導入された配布済み製品応用プログラムを起動して、不正使用防止オーバーレイファイルと解読キーを使用して製品応用プログラムを実行するときに実行する製品応用プログラム一式をロードするためのプロセスが開始される。

このプログラム実行過程を図1に示す。図示されているように、パーソナルコンピュータの使用者が製品応用プログラムの実行をオペレーティングシステムに命令すると、オペレーティングシステムはメインプログラムとローダーセグメントをロードする。ローダーセグメントは他のすべてのプログラム命令に先立って実行される。つぎに、ローダーセグメントは製品応用プログラムの起動を実行し、不正使用防止オーバーレイの存在をチェックする。不正使用防止オーバーレイが導入されていないければ、ローダーセグメントは終了してオペレーティングシステムに戻る。メインプログラムファイルの実行が事前に防止される。不正使用防止オーバーレイが導入されている場合、ローダーセグメントは解読キーを見つけて不正使用防止オーバーレイの解読とロードを行ない、メインプログラムファイルに対して存在しないエグゼキュティブ制御ループプログラム命令ならびに独自の識別および使用許諾制御データを合わせる。解読およびロード過程において巡回冗長検査値が実行され、それが完了すると、不正使用防止オーバーレイが登録用コンピュータからパーソナルコンピュータに伝送されたときに作成された不正使用防止オーバーレイに記憶された巡回冗長検査値と比較される。巡回冗長検査値が失敗に終わると、そのオーバーレイは知らぬ方法によって変更が加えられたものとみなされ、したがって無効とされる。この時点で、ローダーセグメ

## 特表平6-501120 (6)

ントはそのオーバーレイを取り外し、終了してオペレーティングシステムに戻る。したがって、不正変更防止オーバーレイが含まれていない場合と同様に、メインプログラムファイルの実行は、不正変更防止オーバーレイのどの部分が変更されていても、事前に防ぎ止まれる。盗用冗長検査の結果、オーバーレイが変更されていないことが確認されると、ローダーセグメントはオーバーレイを含むメインプログラムファイルの実行を開始し、そして製品応用プログラムが最後に実行される。

不正変更防止オーバーレイは動作可能形態の製品応用プログラムに含めることを要求することにより、盗用者識別と使用許諾制御データはそれ以降動作可能プログラムに常に含められることになる。このようにして、盗用者は不正使用を防止するとともに監視することが出来る。

図1および図2を参照しながら説明したように、本発明によると、登録過程によって、メインプログラムファイルのエグゼクティブ制御ルーブセグメントと使用許諾制御データとを含む不正変更防止オーバーレイファイルが生成される。登録過程が完了すると、この不正変更防止オーバーレイは登録用コンピュータからパーソナルコンピュータに転送される。この不正変更防止オーバーレイは、起動時に不正使用を防止するキー暗号である。なぜなら、エグゼクティブ制御ルーブプログラム命令は、発見なしに自身の使用許諾識別データと使用許諾制御データから分離することとできなければ、盗用者識別と使用許諾制御データも発見なしには変更できないからである。

この不正変更防止オーバーレイファイルは、オーバーレイファイルが生成されると最初に盗用冗長検査値をオーバーレイファイルに記憶させると不正変更防止になるとみなされる。盗用冗長検査値は、プログラム命令と使用許諾データを組み合わせたオーバーレイファイルの内容全体に対して計算される。盗用者データは製品であるので、各々のCRCは製品固有のものになる。記憶されてい

るCRC値が、オーバーレイがロードされるたびにローダーセグメントによって計算された盗用冗長検査値と比較される。これらの盗用冗長検査値が一致しなければ、ローダーセグメントは終了してオペレーティングシステムに戻る。したがって、オーバーレイファイルの内容にどんなかの変更が加えられていれば、記憶されている盗用冗長検査値に該当する変更が行われなくなり、そのオーバーレイファイルは無効になる。つぎに、不正変更防止オーバーレイの内容全体が、盗用冗長検査値の位置が不明になるような方法で暗号化されるので、この値の存在をきつこととてそれを変更することが困難になる。

また、暗号化により、不正変更防止オーバーレイに含まれる特定のプログラム命令をらびに独自の盗用者識別および使用許諾制御データがはつきりしくなる。暗号化は、公開暗号化システムのように暗号化と復号化に別々のキーを使用する構成によって達成される。暗号化ならびに独自の暗号化キーおよび解読キー発出のためのアルゴリズムは登録システム内に蓄積し、したがって盗用者にはアクセスが不可能である。解読キーは、登録システムと登録プログラムシェルスを通じて盗用者のコンピュータに提供される。オーバーレイファイルを解読するためのアルゴリズムはローダーセグメント内にあるので、解読キーと解読アルゴリズムを使用してオーバーレイファイルを解読しその内容を検査することと、困難ではあるが可能である。しかし、内容を複製して、新しい変更されたオーバーレイファイルを暗号化する試みは、暗号化キーに対するアクセスができないために阻止される。私的暗号化キーで暗号化されたオーバーレイファイルだけでは公的解読キーで解読できず、私的キーは盗み取らる場合には用いられないというが、公開暗号化システムの一特徴である。

不正変更防止オーバーレイファイルは、プログラム命令のエグゼクティブ制御ルーブセグメントと、使用許諾の方法と制御に適切な独自の盗用者識別データとを有している。このデータには、

使用許諾の期間、コンピュータの製造番号、コンピュータのモデルの電話番号、そしてその他の情報が含まれる。

ローダーセグメント18は登録目的のサブプログラムであり、これは、ローダープログラムが取り除かれたり迂回された場合、メインプログラムファイルを動作不能にする技術によって製品応用プログラムのメインプログラムファイルに結合される。この結合技術は、特定のプログラム命令と製品応用プログラムのメインプログラムファイル内部に内蔵するプロセスである。これらの内蔵された命令は、盗用者にとっては未知の記憶位置にある特定の値を検査する。ローダープログラムセグメントを実行すると、特定の値がメインプログラムファイルの動作を可能にするのに必要な特定の記憶アドレス位置に記憶される。ローダープログラムセグメントは、その他の後述の如くこの動作を実行する。したがって、ローダーセグメントを取り外したり迂回したりすると、メインプログラムファイルには特定の位置における特定の値が含まれないことになり、そのため動作不能になる。

図の実施例において、登録シェルは、製品応用プログラムの動作可能なデモンストレーション版を含んでいる可能性があるマーケティングパッケージの一部として配布される。デモンストレーション版のプログラムは、ローダーセグメント、デモンストレーション版の解読キー、そしてデモンストレーション版の不正変更防止オーバーレイを含むように設計されている。この場合、不正変更防止オーバーレイには独自の使用許諾データは含まれないが、登録版の製品の構成と表示のデモンストレーションだけを行なうメインプログラムエグゼクティブ制御ルーブが含まれるであろう。デモンストレーション版のエグゼクティブ制御ルーブは、エグゼクティブ制御ルーブの暗号化設計によって暗号化されたプログラムの様々な機能を有している。たとえば、暗号化を提供するデモンストレーションメニューをプログラミングして盗用者を表示することが出来るが、デモンストレーション版のエグゼクティブ

制御ルーブをプログラミングして盗用者を製品登録依頼として解釈して、登録を許可する前に登録することを要求できる。

登録を開始する前に、見込み盗用者はプログラムを実行し、デモンストレーション版が実行されよう。固定しそして図2に示したように、デモンストレーション版の解読キーが使用され、デモンストレーション版のエグゼクティブ制御ルーブがロード、解読、そして実行される。デモンストレーション版が終了すると、見込み盗用者は、盗用者として登録し登録版のプログラムを実行するための一時的な使用許諾を得るようになされる。そして、使用者は前述のようにして登録を行い、図2に示されているプロセスを開始することが出来る。登録要求に応じて、新しいオーバーレイファイル40'と独自の解読キー20'が含まれている盗用ファイルが登録用コンピュータから送られる。盗用プログラムファイルと更新版のプログラムファイルも、出荷ファイルと共に受信される。登録プログラムはデモンストレーション版の不正変更防止オーバーレイ40と解読キー20をそれぞれの登録値40'と20'で置き換える。

登録に続き、盗用者がプログラムを実行すると、プログラム実行過程で登録版の不正変更防止オーバーレイ40が検出されてロードされ、独自の解読キー20'を使用することにより、登録版のエグゼクティブ制御ルーブが解読され実行される。このようにして、デモンストレーション版は完全に動作する登録版に交換される。

プログラムの複製向上版が利用される場合、使用者は同一のプロセスを移動してさらに別の解読キーと、より強化されたエグゼクティブ制御ルーブと追加プログラムファイルを含む別の不正変更防止オーバーレイとを受信して、より強化された版の製品に更新することが出来る。

様々な実施例が、小さな不正変更防止オーバーレイを使用して大きなプログラムの制御を行なうための適切な論理的な技法を使

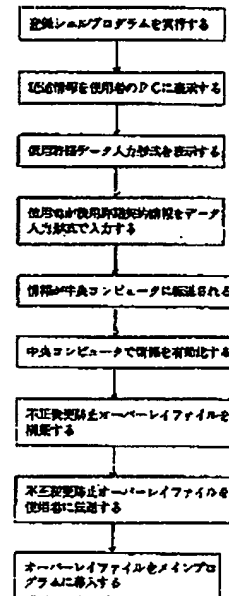
猪表平6-501120 (7)

用することができる。このような技術は、ここにも含まれているように、プログラムの部分あるいはプログラム全体を使用形態変換と結合する形式で記述するための、ここに開示されている方法がもたらす両面利得性の可能性の草をも例である。

上記の知見に照らし合わせ、本発明に鑑み、登録例が可能なことは明らかである。たとえば、本発明は、使用者のコンピュータがその地域の登録用コンピュータに接続され、さらにその登録用コンピュータがそれより広い地域の登録用コンピュータに接続され、というように階層構造的に実施することも可能である。その地域の登録用コンピュータの登録範囲は、その地域の登録用コンピュータとそれより広い地域の登録用コンピュータとの契約に含まれる使用制御データによって制御可能であるであろう。したがって、下記の発明請求の範囲内であれば、本発明と上記明細書に説明されている以外の方法で実施することができる。

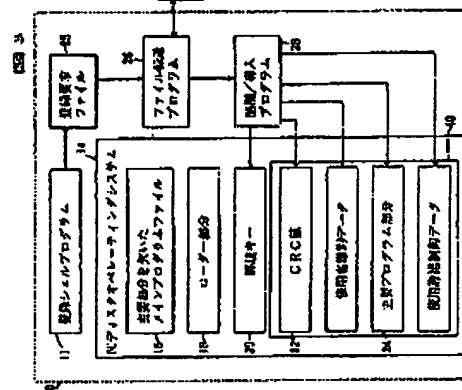
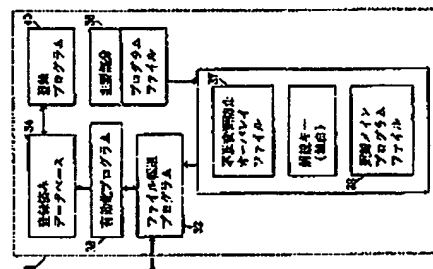
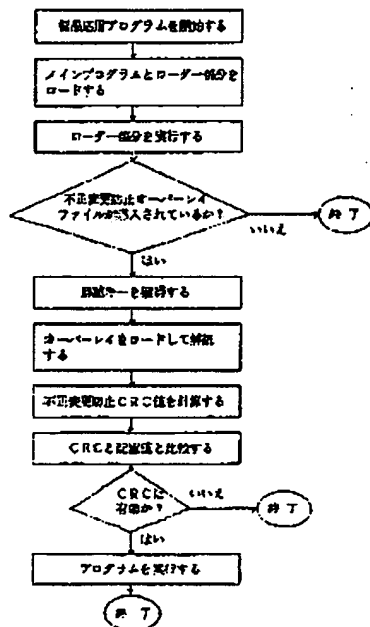
**EX 1**

## 登錄過程



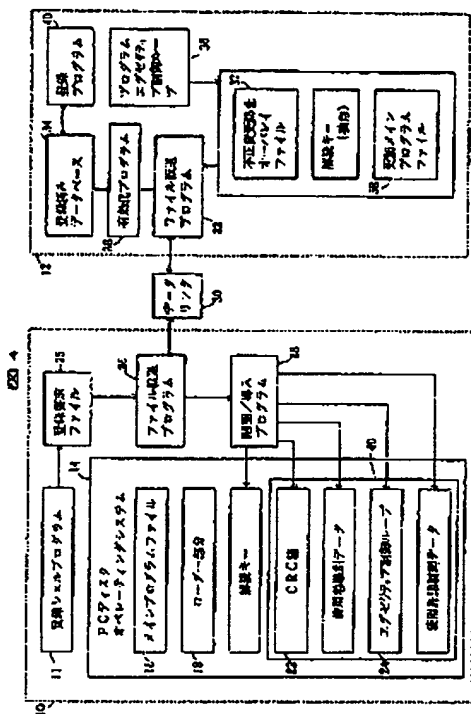
**EX 2**


プログラム実行過程





特 表 平 6-501120 (8)



<div style="text-align: center;">    <b>UNITED STATES DEPARTMENT OF JUSTICE</b>   <b>FEDERAL BUREAU OF INVESTIGATION</b> </div>		<div style="text-align: right;"> <b>Form No. 101 (Rev. 1-25-60)</b> </div>	
<b>1. NAME OF THE PERSON OR ENTITY</b> <span style="float: right;">(b) (7)(C) - (b) (7)(D)</span>			
<b>2. ADDRESS OF THE PERSON OR ENTITY</b>		<b>3. CITY, STATE, AND ZIP CODE</b>	
<b>4. DATE OF THE INFORMATION</b>		<b>5. DATE OF THE INFORMATION</b>	
<b>6. NAME OF THE PERSON OR ENTITY</b>			
<b>7. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>8. CITY, STATE, AND ZIP CODE</b>			
<b>9. DATE OF THE INFORMATION</b>			
<b>10. DATE OF THE INFORMATION</b>			
<b>11. NAME OF THE PERSON OR ENTITY</b>			
<b>12. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>13. CITY, STATE, AND ZIP CODE</b>			
<b>14. DATE OF THE INFORMATION</b>			
<b>15. DATE OF THE INFORMATION</b>			
<b>16. NAME OF THE PERSON OR ENTITY</b>			
<b>17. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>18. CITY, STATE, AND ZIP CODE</b>			
<b>19. DATE OF THE INFORMATION</b>			
<b>20. DATE OF THE INFORMATION</b>			
<b>21. NAME OF THE PERSON OR ENTITY</b>			
<b>22. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>23. CITY, STATE, AND ZIP CODE</b>			
<b>24. DATE OF THE INFORMATION</b>			
<b>25. DATE OF THE INFORMATION</b>			
<b>26. NAME OF THE PERSON OR ENTITY</b>			
<b>27. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>28. CITY, STATE, AND ZIP CODE</b>			
<b>29. DATE OF THE INFORMATION</b>			
<b>30. DATE OF THE INFORMATION</b>			
<b>31. NAME OF THE PERSON OR ENTITY</b>			
<b>32. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>33. CITY, STATE, AND ZIP CODE</b>			
<b>34. DATE OF THE INFORMATION</b>			
<b>35. DATE OF THE INFORMATION</b>			
<b>36. NAME OF THE PERSON OR ENTITY</b>			
<b>37. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>38. CITY, STATE, AND ZIP CODE</b>			
<b>39. DATE OF THE INFORMATION</b>			
<b>40. DATE OF THE INFORMATION</b>			
<b>41. NAME OF THE PERSON OR ENTITY</b>			
<b>42. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>43. CITY, STATE, AND ZIP CODE</b>			
<b>44. DATE OF THE INFORMATION</b>			
<b>45. DATE OF THE INFORMATION</b>			
<b>46. NAME OF THE PERSON OR ENTITY</b>			
<b>47. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>48. CITY, STATE, AND ZIP CODE</b>			
<b>49. DATE OF THE INFORMATION</b>			
<b>50. DATE OF THE INFORMATION</b>			
<b>51. NAME OF THE PERSON OR ENTITY</b>			
<b>52. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>53. CITY, STATE, AND ZIP CODE</b>			
<b>54. DATE OF THE INFORMATION</b>			
<b>55. DATE OF THE INFORMATION</b>			
<b>56. NAME OF THE PERSON OR ENTITY</b>			
<b>57. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>58. CITY, STATE, AND ZIP CODE</b>			
<b>59. DATE OF THE INFORMATION</b>			
<b>60. DATE OF THE INFORMATION</b>			
<b>61. NAME OF THE PERSON OR ENTITY</b>			
<b>62. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>63. CITY, STATE, AND ZIP CODE</b>			
<b>64. DATE OF THE INFORMATION</b>			
<b>65. DATE OF THE INFORMATION</b>			
<b>66. NAME OF THE PERSON OR ENTITY</b>			
<b>67. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>68. CITY, STATE, AND ZIP CODE</b>			
<b>69. DATE OF THE INFORMATION</b>			
<b>70. DATE OF THE INFORMATION</b>			
<b>71. NAME OF THE PERSON OR ENTITY</b>			
<b>72. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>73. CITY, STATE, AND ZIP CODE</b>			
<b>74. DATE OF THE INFORMATION</b>			
<b>75. DATE OF THE INFORMATION</b>			
<b>76. NAME OF THE PERSON OR ENTITY</b>			
<b>77. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>78. CITY, STATE, AND ZIP CODE</b>			
<b>79. DATE OF THE INFORMATION</b>			
<b>80. DATE OF THE INFORMATION</b>			
<b>81. NAME OF THE PERSON OR ENTITY</b>			
<b>82. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>83. CITY, STATE, AND ZIP CODE</b>			
<b>84. DATE OF THE INFORMATION</b>			
<b>85. DATE OF THE INFORMATION</b>			
<b>86. NAME OF THE PERSON OR ENTITY</b>			
<b>87. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>88. CITY, STATE, AND ZIP CODE</b>			
<b>89. DATE OF THE INFORMATION</b>			
<b>90. DATE OF THE INFORMATION</b>			
<b>91. NAME OF THE PERSON OR ENTITY</b>			
<b>92. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>93. CITY, STATE, AND ZIP CODE</b>			
<b>94. DATE OF THE INFORMATION</b>			
<b>95. DATE OF THE INFORMATION</b>			
<b>96. NAME OF THE PERSON OR ENTITY</b>			
<b>97. ADDRESS OF THE PERSON OR ENTITY</b>			
<b>98. CITY, STATE, AND ZIP CODE</b>			
<b>99. DATE OF THE INFORMATION</b>			
<b>100. DATE OF THE INFORMATION</b>			

## フロントページの続き

(51) Int. Cl.<sup>8</sup> H 0 4 L 9/12

(61)指定国 EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IT, LU, NL, S E), CA, JP